

# Construction

## Cyber risk exposures and solutions

Construction organisations are a target for cyber criminals with motives of financial gain via theft of confidential information or money. Cyber is a broad risk that organisations face by virtue of their reliance on information technology, connectivity and automated processes. In an increasingly punitive legal and regulatory environment, and with more frequent contractual requirements for cyber liability insurance, forward thinking companies are taking proactive steps to explore and transfer cyber risk.

Numerous factors contribute to an organisation's cyber risk profile, including: action by employees, system and programme errors, security measures, industry, nature and quantity of data collected, political or strategic significance and reliance on technology.

### Cyber risk considerations for construction organisations:

- ▶ Gathering, maintaining, disseminating or storage of private information
- ▶ High dependency on electronic processes or computer networks
- ▶ Contingent bodily injury and property damage resulting from cyber incidents
- ▶ Increased attention of hackers due to high profile buildings or projects, including government buildings, infrastructure (water and power) and military projects
- ▶ Utilisation of "the cloud" exposes contractors to liability ranging from data security, network outages, and regulatory compliance issues
- ▶ Reliance on or operation of critical infrastructure
- ▶ Subject to regulatory statutes
- ▶ HIPAA risk associated with medical facility construction
- ▶ Dependence on vendors, independent contractors or additional service providers
- ▶ Vendor held information:
  - Building Information Modelling (BIM) programmes
  - Laptops and portable devices (iPhones, iPads, etc.) to access systems from third party locations such as job sites or hotels

### Potential cyber incidents for construction organisations:

- ▶ Hacker access to construction data, disrupting not only operationally, but also through the physical destruction of data, servers and infrastructure, or by threatening the safety of people onsite
- ▶ Network interruption resulting in lost business income
- ▶ Intentional acts committed by rogue employees
- ▶ Ransomware attacks

### We're here to empower results

**Scott Davies**  
Cyber Construction Industry Expert  
+971 4389 6412  
[scott.davies@aon.ae](mailto:scott.davies@aon.ae)

**Shannan Fort**  
Cyber Insurance Leader  
Global Broking Centre  
+44 (0)20 7086 7135  
[shannan.fort@aon.com](mailto:shannan.fort@aon.com)

**David Molony**  
Cyber Risk Leader  
Global Risk Consulting  
+44 (0)777 5227008  
[david.molony@aon.co.uk](mailto:david.molony@aon.co.uk)

**Spencer Lynch**  
Cybersecurity Leader  
Stroz Friedberg  
+44 (0)20 7061 2304  
[slynch@strozfriedberg.co.uk](mailto:slynch@strozfriedberg.co.uk)

**Vanessa Leemans**  
Chief Commercial Officer  
Cyber Solutions EMEA  
+44 (0)20 7086 4465  
[vanessa.leemans@aon.co.uk](mailto:vanessa.leemans@aon.co.uk)

[aon.com/cyber](https://aon.com/cyber)  
[strozfriedberg.com/resource-center](https://strozfriedberg.com/resource-center)

# Scope of traditional cyber coverage available in the insurance marketplace:

## Third party coverage elements

- **Security and privacy:** defence costs and damages suffered by others resulting from a failure of computer security, including liability caused by theft or wrongful disclosure of confidential information, unauthorised access, denial of service attack or transmission of a computer virus
- **Regulatory defence and fines:** defence costs for proceedings brought by a governmental agency in connection with a failure to protect private information and / or a failure of network security
- **Media liability:** defence costs and damages suffered by others for content-based injuries such as libel, slander, defamation, copyright infringement, trademark infringement, or invasion of privacy
- **PCI fines and assessments:** defence costs for investigations brought by the Payment Card Industry (PCI) in connection with a failure to protect private information and / or network security

## First party coverage elements

- **Breach response costs associated with:** breach notification, including the hiring of outside law firms and public relations consultants, forensic costs, credit monitoring / protection, notification hot-line / call centre, identity theft resources
- **Network business interruption:** loss of income and extra expense due to network security failure
- **Dependent business interruption:** reimburses the insured for actual lost net income and extra expense incurred when the insured's service provider's computer system is interrupted / suspended due to a failure of network security
- **System failure business interruption:** coverage for business interruption due to an unintentional or unplanned system failure not caused by a failure of network security
- **Data restoration:** costs to restore / recreate data / software resulting from network security failure
- **Cyber extortion:** reimburses the insured for expenses incurred in the investigation of a threat and any extortion payments made to prevent or resolve the threat

## Aon has successfully negotiated the following key coverage enhancements (subject to market agreement per individual risk):

- |   |  |
|---|--|
| • Full limits for incident response and costs associated with breach notification | • Supply chain business interruption coverage                      |
| • Broad definition of computer system   | • Cost of spoilage – replacement of materials that are transferred |
| • Coverage for cyber terrorism  | • Bricking coverage – replacement costs for IoT devices            |
| • Deletion of the unencrypted device exclusion                                    | • Delay in delivery/delay in performance coverage                  |
| • No failure to patch exclusion   | • Environmental liability coverage                                 |

# Our approach

## Adopting a risk based cyber insurance strategy

Aon's cyber capabilities can support organisations in embracing a risk based approach through:

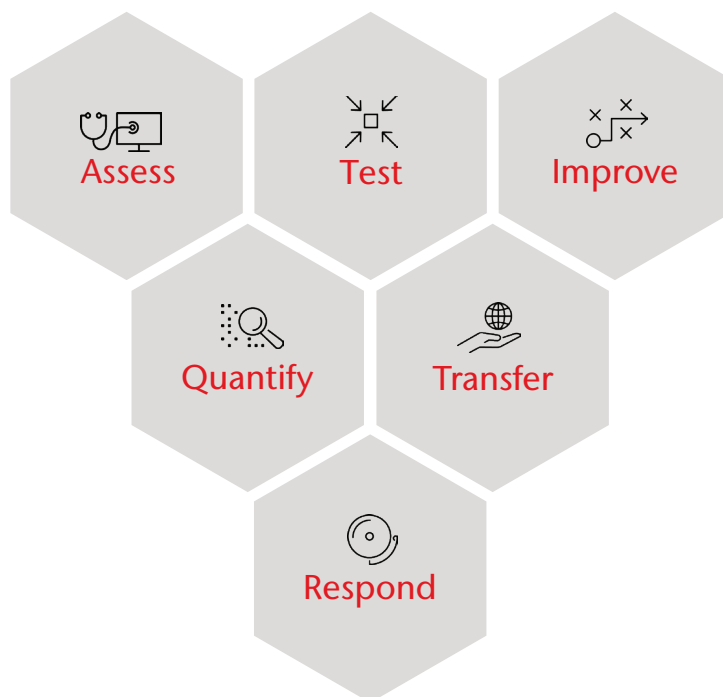
- *Cyber Assessment* - an enterprise wide approach to cyber security risk that provides a detailed view into an organisation's unique technology profile and threat landscape, with a focus on facilitating risk quantification and insurability.
- *Cyber Impact Analysis* - a data driven analytical framework supporting organisations to optimise their resilience strategy through mitigation and transfer. Existing risk financing strategies can also be enhanced through modelling cyber loss scenarios and stress testing current limits.

## Cyber innovation

- *Aon Cyber Enterprise Solution™* - a policy which broadens the scope of cyber coverage to include: property damage arising out of a network security breach, business interruption and extra expense coverage arising out of a systems failure, contingent network business interruption for IT vendors and the supply chain, cyber terrorism coverage, etc.
- *Aon's GDPR Protect Solution* - a modular risk management solution that helps organisations manage financial, regulatory and legal risks associated with processing personal data under the EU General Data Protection Regulation (GDPR).

## Our cyber resilience framework

Aon and Stroz Friedberg offer a full range of services to help you approach cyber as an enterprise risk and achieve cyber resilience.



# Client story



Stroz Friedberg worked with a global engineering and design consultancy operating across 23 locations, who were concerned about how a cyber incident could impact their critical technology and operations.

---



To understand the risk profile of the organisation, we carried out a detailed cyber security and vulnerability assessment of the client's system architecture. This was accomplished by looking at severe and plausible incident scenarios the engineering consultancy might face and a quantification of the potential financial losses.

Following the cyber risk assessment and quantification, the team was also able to recommend and implement a wide range of cybersecurity optimisations through:

- Penetration and red team testing
  - System architecture evaluation and improvement planning
  - Board-level workshops and planning
  - Review of existing cyber insurance policy compared to the total cost of risk
- 



By approaching cyber as an enterprise risk, the global engineering and design consultancy firm gained a comprehensive understanding of the impact of a cyber incident and were able to address the vulnerabilities in their critical technology and operations.